DEPARTMENT OF THE ARMY

**HEADQUARTERS, U.S. ARMY MEDICAL DEPARTMENT CENTER AND SCHOOL
AND FORT SAM HOUSTON
2250 STANLEY ROAD
FORT SAM HOUSTON, TEXAS 78234-6100**

**REPLY TO
ATTENTION OF**

MCCS-BIM   26 NOV 2002

MEMORANDUM FOR SEE DISTRIBUTION

SUBJECT: Installation Information Management Policy 25-07, Firewalls

1. REFERENCES**.** References are provided in Appendix A.

2. PURPOSE. To establish the operational firewall policy for the Fort Sam Houston (FSH) network environment. This document is in concert with the Defense Information Technology Security Certification and Accreditation Process (DITSCAP) accreditation document.

3. SCOPE. This policy applies to all FSH Local Area Network (LAN), Wide Area Network (WAN), and dial-up connections to and from the FSH network and assigns the responsibility to the Information Technology Business Center (ITBC) for planning, acquiring, implementing, and maintaining firewalls. This policy applies to all existing and future firewall implementations for both government and non-government organizations on FSH.

4. POLICY. All connections between the FSH network and equipment outside the Garrison infrastructure shall be routed through ITBC's installation firewall. Bypassing or defeating the installation firewall system using modems, leased commercial circuits, Application Service Providers, or network tunneling software to connect directly to outside networks is not permitted.

   a. To insure compliance with this policy ITBC will:

      (1) Determine the need for re-accreditation for FSH networks firewall configurations when changes or modifications are necessary.

      (2) Ensure only Certified Network or Firewall Administrators perform configuration functions.

      (3) Perform Information Assurance Vulnerability Assessments of the effectiveness of the FSH firewall configuration on a periodic basis.

      (4) Consider requests for addition, deletion, and changes to Internet Protocol addresses, Domain Name Service, and FSH firewall connectivity.

      (5) Ensure all firewalls on FSH are operated on dedicated hardware with sufficient capacity to operate in a high-performance environment.

MCCS-BIM
SUBJECT: Installation Information Management Policy 25-07, Firewalls

(6) Assess the firewall configuration profile on a periodic basis using FSH approved network security tools and manual procedures.

  b. The FSH Firewall Administrators will:

(1) Comply with applicable DOD and DA guidance/directives and this firewall policy.

(2) Ensure no new services nor protocols are made operational without prior approval from ITBC Security Division.

(3) Perform backups of the firewall configuration whenever configuration changes are made.

(4) Monitor the firewall for breaches and attempts to circumvent firewall or network security.

(5) Report security related incidents to the ITBC Information Assurance Manager.

(6) Within 30 days after effective date of this policy, provide a report to the ITBC Security Division on any existing firewalls. Information will include:

(a) Make and model of the firewall.

(b) Operating system and version.

(c) A copy of the configuration file.

(d) Diagram outlining physical placement of the firewall and its protected network location.

(e) Firewall administrator POC and telephone number.

(7) Provide future firewall configuration changes to the ITBC Security Division for review and approval prior to implementation. The ITBC will process routine changes within 2-3 workdays from receipt and urgent changes within 1 workday.

5. EXPIRATION. This policy expires 2 years from the implementation date.

MCCS-BIM
SUBJECT: Installation Information Management Policy 25-07, Firewalls

6. The point of contact is Mr. Ralph Coogan, Chief, Security Division, Information Technology Business Center, 221-8639, or email address (ralph.coogan@us.army.mil).

Encl   DARREL R. PORR
as   MG, US Army
                                                        Commanding

DISTRIBUTION:
A, B, Plus:
30 – MCCS-BHR-A

Appendix A

References:

Title 36, Code of Federal Regulations, Chapter 12, "National Archives and Records Administration," Subchapter B, Records Management, July 1, 1999.

DOD Directive 5015.2, Records Management Program, April 11, 1997.

DOD Directive 5200.28, Security Requirements for Automated Information Systems, and all amendments, March 21, 1988.

DOD Directive 7740.1, Information Resources Management Program, and all amendments, June 20, 1983.

DOD Directive 7950.1, Automated Data Processing Resources Management, and all amendments, September 29, 1980.

DOD Instruction 5210.74, "Security of DOD Contractor Telecommunications," June 26, 1985.

Public Law 100-235, Computer Security Act, and all amendments, January 8, 1988.

OMB Circular No. A-130, Management of Federal Information Resources and all amendments, February 8, 1996.

National Institute of Standards and Technology, NIST publication 800-7, Introduction to Internet Firewalls, 1994. http://csrc.nist.gov/publications/nistpubs/800-7/node155.html.

NIST94a, NIST. Guideline for the Use of Advanced Authentication Technology Alternatives. Federal Information Processing Standard 190, National Institute of Standards and Technology, September 1994.

NIST94b, NIST. Reducing the Risk of Internet Connection and Use. CSL Bulletin, National Institute of Standard and Technology, May 1994.

DeCA Directive 35-12, "Network Security & Firewall Policy," February 18, 2000.

RFC1244, Paul Holbrook and Joyce Reynolds. RFC 1244: Security Policy handbook. Prepared for the Internet Engineering Task Force, 1991.

RFC2196, B. Fraser, Editor. SEI/CMU. RFC 2196: Site Security Handbook. Network Working Group. Multiple contributing authors. September 1997.

Carnegie Melon University Software Engineering Institute: CERT Security Improvement Modules, Design the Firewall System, 1999. http://www.cert.org/security-improvement/.

Appendix A

Computer Security Handbook, 3rd Edition, Hutt, A. E., Bosworth, S.; Hoyt, D.B., John Wiley & Sons, Inc. 1995.

International Computer Security Association (ICSA) Guide to Cryptography, Nichols, R. K., McGraw-Hill, 1999.

Defending Your Digital Assets Against Hackers, Crackers, Spies & Thieves, Nichols, R.K.; Ryan, D.J.; Ryan, J.J.C.H., RSA Press/McGraw-Hill, 2000.

Hacking Exposed, McClure, S.; Scambray, J.; Kurtz, G., Osborne/McGraw-Hill, 1999.